



IDENTITY THEFT

The latest criminal trend has put the media in a frenzy, but how exactly do fraudsters steal your identity?

Simon Edwards looks at the techniques used and explains how you can prevent it happening to you

Identity theft is big news. TV adverts show Alistair McGowan spending your cash. Newspapers report that this type of crime has spiralled in popularity. And surveys scream that the majority of the British public is worried about having their identity stolen.

For many of us, identity theft is a phrase that instils fear, but what exactly does it mean? Does the digital age make it easier to have your identity stolen? We've investigated the truth behind the hype, drilling down into the figures, headlines and reports to bring you the low-down on what identity theft is, how it affects you, how criminals do it and what you can do to stop them.

WHAT IS ID THEFT?

Identity theft involves a criminal gaining access to information and documents about a victim. They can then masquerade as the victim to access bank accounts, apply for credit cards and loans, and use any number of other financial services.

The victim could be a member of the public picked at random or even a deceased individual. The Credit Industry Fraud Avoidance System (CIFAS) claims that the largest single form of

identity theft is from dead people, which accounts for around 30 per cent of this type of crime. As we'll see, though, even stealing the identities of the dead is not a victimless crime.

The end result of a successful identity theft is that an innocent person ends up facing a large bill and, if they are unlucky, a large bailiff. Their credit rating could be damaged, affecting their ability to take out legitimate loans, transfer their mortgage, or organise insurance. If the police get involved victims could spend time helping with enquiries.

Being the victim of identity theft is likely to cause emotional distress rather than a large debt. It's important to remember that, ultimately, you are not liable for the behaviour of the criminal who is pretending to be you. However, you will still want to avoid this situation, if just for an easy life. With a bit of effort you can help prevent your details falling into the hands of identity thieves and reduce the chances that you will fall foul of them.

HOW COMMON IS IT?

Identity theft is not very common in the UK. Although the figures are rising, fraud committed by ID thieves still rates low on the charts. In 1999 there

were 20,000 recorded attempts of identity theft in the UK, which rose to 101,000 in 2003. Although final figures for 2005 were not available as we wrote this article, conservative estimates indicate a total of 144,000 cases. These are attempted thefts of identity, not necessarily successful ones.

Considering that the UK has a population of around 60 million, we can expect one attempt at an identity theft for every 600 people alive in the country during 2005. There are no figures available to say how many of those attempts will succeed, but CIFAS estimates that financial institutions spot 90 per cent of attempted frauds. Even if every attempt to steal an identity succeeded, most of the thieves would be thwarted when trying to commit a fraud.

The probability of being affected by an identity theft is harder to calculate, because 30 per cent of identity theft victims are dead. If we include them, the probability increases to one in 418 people. If you count one member of the deceased's next of kin as a victim, then this is a more accurate figure.

HOW DO THEY DO IT?

In order to protect yourself you need to know how the criminals steal your information. Here are the



SHREDDERS

Public awareness of identity theft is at an all-time high, and shredder sales surged by up to 15 per cent in 2005. So should you buy one, and what features should you look for?

There are a number of things you should look out for before parting with your cash. Possibly the most important is the type of cut that the shredder makes. Strip-cut shredders turn pages into long, thin strips. In some cases these can, with patience and sticky tape, be reconstructed. Cross-cut shredders chop the sheets into little pieces, which are virtually impossible to put back together.

Some cross-shredders handle CDs and credit cards, too. The Dahle 20082 is one such model and costs £69 plus VAT. The Olivetti Privacy 6000c is a dedicated CD shredder that will cross-cut CDs, DVDs, credit cards, floppy disks and paper. It costs the same. Both are available from ABT (www.abt-shredders.co.uk).

Shredders sometimes come with a security rating, from one to five. Models rated at one are suitable for everyday documents. Confidential data, which these days we take to mean anything, should be shredded with a level three shredder. Top-secret documents can be turned to dust with a level five shredder. Both models mentioned above have a level three rating.

It's best to shred your own documents, rather than employing a company to do it for you. Not only is it cheaper, but you can't be sure how long your paper will be stored before it is destroyed, if at all. We've heard stories of cowboy companies dumping unshredded sensitive documents from multiple clients in a warehouse that was accessible by anyone. This makes an attractive target for thieves.

You're best off putting shredded paper in your bin or recycling box. If it's cross-cut, it can also be used as compost. Only the most dedicated ID thief will attempt the task of re-assembling cross-cut documents, particularly if they are mixed in with kitchen waste.

Owners of domestic furnaces have access to the ultimate document disposal method. The truly paranoid should stir up the ashes before dumping them.



▲ The Olivetti Privacy 6000c destroys CDs, credit cards and floppy disks as well as paper documents



Look out for skimming devices such as the one above on cash machines. If you're in any doubt, use another cashpoint

most common ways for people to gain information and assume alternative identities.

• **ROBBING THE DEAD** Spies, terrorists and other criminals have been stealing identities to use for cover for years. In his 1972 novel *The Day of the Jackal*, Frederick Forsyth described how simple it was to obtain a fake passport using the details of a dead person. The assassin in the book searched a graveyard for a headstone of a child with whom he shared a similar year of birth. He then applied for a birth certificate in that child's name and used that to obtain a passport.

In November 2005 Christopher Edward Buckingham, who also claimed to be the Earl of Buckingham, was found to have been living a lie for 22 years, having used the 'Jackal' technique of obtaining a birth certificate of a dead child. He was sentenced to 21 months in jail for obtaining a passport by deception. A routine check of passport records found that his identity conflicted with a death certificate.

The loophole that allows this is still open, although a planned computerised system for recording births and deaths will help prevent people stealing the identities of the dead in the future. Frederick Forsyth raised the issue again in 2003, and the Office of National Statistics confirmed to us that, two years on, the loophole still exists. It has been over 30 years since Forsyth first publicised the problem. A computerised system aimed at solving it is still in development.

• **MAIL THEFT** If you have ever lived in a shared house or in flats where post is stored communally, you'll appreciate how easy it is to obtain other people's mail. That means access to their utility bills, credit card and bank account statements and other sensitive documents.

A dishonest person living with or near you can intercept your mail and make applications for further services using your details. If successful, they can steal the responses sent by the new companies. Eventually they could change your customer details so that your mail is sent to a different address.

Some fraudsters go one step further by forwarding all their victims' mail to a different address. Despite documented cases where this has happened, the Royal Mail told us that "ID is required to set up a redirection. When a redirection is applied for, or if any changes are made to a redirection, Royal Mail notifies the occupant of the address from which the mail is to be redirected."

Of course, if a fraudster already has your ID they can start a redirection themselves. If they also have access to your mail, they can prevent you receiving notification.

Mail theft is certainly easier if the thieves have access to your current or previous address. If you don't use mail redirection when you move, credit card offers and personal mail may fall into the hands of scammers. In one case documented by CIFAS, a couple moved house and later discovered that the new occupants had re-registered them on the Electoral Register and applied for a credit card. They ran up a bill of £2,500, which was discovered only when the victims applied for a card themselves and were declined.

• LOTTERY WINS AND OTHER SCAMS

If someone contacts you with the good news that you've won a lottery that you don't remember entering, or that you're the beneficiary of some bonds, be suspicious. If you are then asked to supply personal details, such as your date of birth and mother's maiden name, you can be sure it's a scam designed to steal your identity.

Replying to such letters will allow fraudsters to attempt to apply for credit cards and, in one case we've heard of, also gain access to personal bank accounts.

• RUBBISH BINS, ROBBERY AND SKIMMING

What do you do with your most valuable stash of personal information? Throw it in the bin, usually. Going through rubbish bins is a popular *modus operandi* for identity thieves. All those old bank statements, shopping receipts, credit card and utility bills can help them apply for credit accounts in your name.



Muggers, burglars and pickpockets can earn themselves a bonus by abusing personal details they find in recently stolen wallets and purses. Criminals working at shops and restaurants can use a device called a skimmer to copy your credit or debit card's details. The magnetic reader allows them to clone your card and start spending on your account. Handheld skimmers, or devices attached to ATMs, are often used.

• **INTERNET SCAMS** Last but not least, it is possible for thieves to steal your personal details using the internet. Although it is technically feasible for a hacker or computer virus to infiltrate your PC and grab your account details, it is far more likely that you will receive fraudulent emails purporting to come from a company with which you have an account. These 'phishing' attempts request that you reply with personal details. They often appear legitimate because fraudsters use security holes in email and web browser software to make their emails seem real.

Internet users are also at risk from electronic versions of the other techniques listed above. For example, if your email password is compromised, an attacker could gain personal information by checking your email. You can receive lottery scam emails or have your notebook (complete with accounts software) stolen. You are at risk if you store personal details on your computer, although less than if you routinely throw your credit card receipts into a high street rubbish bin.

In August 2005 security firm Sunbelt Software claimed it had stumbled on a server containing "a large number of usernames, passwords, telephone numbers, credit card and bank account numbers, and other personal information". This information was gathered by a keylogging program, which also steals details saved to the hard disk by Internet Explorer's AutoComplete feature. Keyloggers and other Trojans can infect systems via viruses, worms and spyware. In the latter case, just visiting the wrong website can be enough to infect your system.

PREVENTATIVE MEASURES

To protect yourself from identity theft you need to make some changes to your personal routine. At the very least, you should be aware of the potential value your personal information has to criminals. A gas bill might not seem like the keys to the

kingdom, but a collection of informational snippets can build up into a useful database. Once your mind is set on securing your personal data, you should follow our guidelines and reduce the risk of criminals abusing your ID.

PC PROTECTION

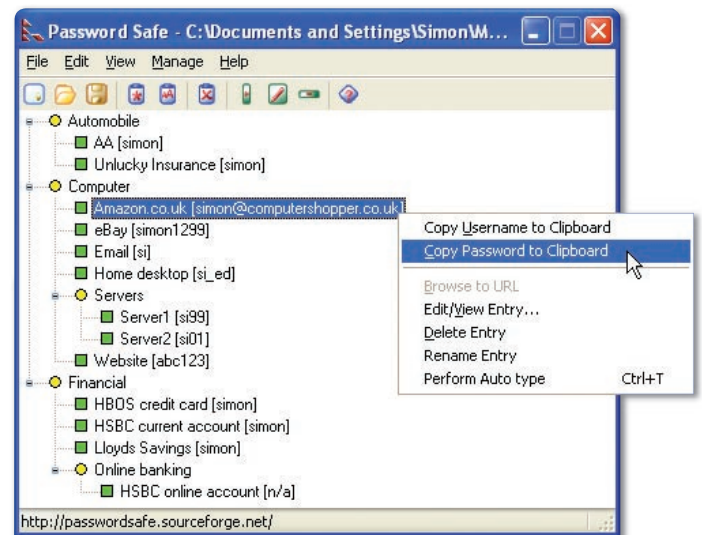
Your computer probably holds lots of personal information. If you bank online you will type in some form of password. Anything you type or store in a file on your internet-connected PC can be read by an attacker unless you take precautions. A good anti-virus program, such as Kaspersky Lab Anti-Virus Personal 2005, and a personal firewall will go a long way to preventing keyloggers and backdoors leaking your information on the internet.

Encryption can also help (see *Advanced Windows, Shopper* January 2006), particularly when used with files created by accounts software. That way, if someone steals your computer, finds an old, discarded hard disk or hacks into your computer, they still face a significant obstacle to getting your important information.

Personal digital assistants (PDAs), smartphones and other portable electronic organisers can also hold personal data. Use password protection at the very least. If you don't, and you lose your device, someone could find out a lot about you.

PASSWORDS AND SECURITY

Computer passwords are always tricky – you have to remember many different passwords for online banking, email, your work computer, possibly your home PC too, as well as any web-hosting services, access to online mobile phone pages, chat forums and so on. But you can't use the same one all the time – otherwise, should someone find it out, they will be able to own your life easily.



▲ Password Safe is a free program that automatically encrypts all your passwords. You can get it from <http://passwordsafe.sourceforge.net>

Possibly the simplest thing you can do is list every password you have on a sheet of paper and lock it in a filing cabinet. There is a risk that someone could break into that cabinet or you might leave it unlocked one day, but this is still better than keeping little notes in your wallet or on an unprotected handheld computer.

If you want to manage passwords using your computer, don't ever allow Windows, your web browser or any other program to remember your password. Entering passwords manually is inconvenient, but there are plenty of programs around that can dig out saved passwords from Windows computers.

Instead of keeping a plain list of passwords on your hard disk, use a removable disk such as a CD or USB key. If you want the best protection, encrypt the list using software such as PGP, Steganos Security Suite 7 (see *What's New, Shopper* February 2005) or the free, but harder to use, GnuPG. Password Safe is a very useful program that is designed specifically for protecting passwords and it is free. It keeps a database of account details for different services and encrypts them automatically. You can download copies for Windows PCs and Pocket PCs from <http://passwordsafe.sourceforge.net>.

When you set up an account at a bank, a utility company or many other organisations, you'll often be asked to provide answers to some security questions. Invariably this will include your mother's



▲ Removable media such as CDs or USB keys are an ideal place to store passwords, although for complete protection you should also encrypt them

DON'T FEAR THE KNOCK ON THE DOOR

If your identity has been stolen and used for fraudulent purposes, you might be worried about a call from the bailiffs or the police. But how likely is it that Big Frank will take the TV or the police will batter down your door at 3am?

The National Crime Squad assured us that it approaches matters on a "case-by-case basis that involves intelligence work and investigation". They won't go around bashing in doors on morning raids without putting you under surveillance first, and they've got to be pretty sure you really are a drug baron before spending money and manpower trying to apprehend you.

Debt-reclamation agencies might appear on your doorstep, but only after you've received

numerous letters. If you start getting final demands for things you haven't bought, you can save yourself a lot of trouble by responding to them rather than ignoring them. Let the agency know that it's not your problem.

If a bailiff does turn up on your doorstep, be aware that he is not allowed to break into your house. If you leave a door open he can walk through it, and open windows are fair game too. If you've signed a walk-in agreement the rules change and he can make a forceful entry. However, walk-in agreements can only be made if the bailiff has previously made a peaceful entry. So if you never allow a bailiff in, you should be safe.



maiden name. The sad truth is that employees can be corrupt, or corruptible. Or plain stupid. If an employee collects or passes on details such as customers' mothers' maiden names, these can be reused by a criminal who wants to impersonate you. And it will work with every company to which you gave the same answer.

It makes more sense to provide randomly invented answers to such security questions. It's easy to solve the problem of remembering which answer you gave to which company. Create an entry on your password list, or in the Password Safe database, for every service that you've signed up for and, as well as your username and password, list your answers to the security questions.

MONITOR YOUR CREDIT

Keep an eye on your bank and credit card statements. If you see any unusual activity, report it to the company immediately. The UK's Association for Payment Clearing Services (APACS) says that identity theft accounted for £16m worth of fraud in the first half of 2005.

The majority of plastic card fraud is due to so-called card not present (CNP) fraud, where an unauthorised person has bought online, via mail order or over the telephone using someone else's card details. This doesn't really count as identity theft, but it's still a threat worth mentioning, particularly as CNP-related fraud rose by 29 per cent in just one year. In January to June 2004 it accounted for over £70m, but between January and June 2005 over £90m was stolen.

Checking your records with CIFAS will alert you if someone has tried or is trying to steal your identity. When a CIFAS member, such as a credit card company, detects a suspected fraud it will place a warning against the name and address of the applicant. If someone is trying to apply for a credit card in your name, the warning will appear on your record. CIFAS is at pains to point out that this is not an accusation that you are a fraudster, just that someone has tried to use your details.

If there is a warning next to your name, other companies that have access to the database will

take extra precautions when handling applications from that person. The warning will also affect an address. This is why, if you live in rented properties, you may occasionally find it tricky to get a credit card. If your address has a warning against it, perhaps because of a fraudster who has either lived there before or who has simply used the address in his schemes, you may experience delays in your applications.

You can find out if there is a warning by exercising your rights under the Data Protection Act, which allows you to seek access to any data held by CIFAS. A request costs up to £10. Additionally, you are allowed to demand a copy of your credit file. This costs just £2. According to CIFAS, "where a CIFAS-participating agency is also a credit reference agency, this credit file includes all the data held by the credit reference agency about the individual and any CIFAS data". You can contact CIFAS at www.cifas.org.uk.

If you keep being declined credit, it may simply be because your credit rating is not good enough. In our experience that is more likely to mean that you've never been in debt than anything else. CIFAS clearly states that its members "are not allowed to refuse applications simply because a CIFAS warning is present".

DECEASED FRAUD

Despite the apparent ease with which fraudsters can assume the identities of the dead, you can help protect the identity of your deceased relatives. More importantly, protecting them may also protect surviving but vulnerable partners. CIFAS told us of one woman who found that her dead husband's identity was stolen at least 13 times. In another case, relatives received a bill for a debt in the name of a deceased individual. They paid up, before discovering that the debt did not actually belong to their family.

Relatives or executors of the deceased can place an entry in the CIFAS Protective Registration. This includes the deceased person's address. According to CIFAS, "the service protects the identities registered with it by flagging to over 240 CIFAS member companies (virtually the whole financial services industry) that the identity is at risk of being misused".

To do this you need to call 08700 102091 and pay a fee of £11.75 including VAT. You'll also need a copy of the death certificate.

PROTECTIVE REGISTRATION

If your personal details have been stolen you can place a warning against your own address to alert financial companies that a fraudster could be about to impersonate you. That way, when any would-be thief tries to order a card in your name, they should find it more difficult to conclude the deal.



Always keep an eye on your credit card when paying for goods. The card should be swiped once, on the till or a portable chip and PIN device

To do this, contact the fraud prevention and credit reference agency Equifax on 08700 100583 or at www.equifax.co.uk. You'll need your name, address, date of birth, the names of other people living at your house, their dates of birth, home and work telephone numbers, a crime reference number (if you were mugged or burgled) and a reason for placing the warning.

MAIL INTUITION

If you move house, you should set up mail redirection with Royal Mail, as well as notifying every company with which you have an account. Don't forget store cards, car recovery services and other companies that you might not deal with on a weekly or monthly basis. Royal Mail told us that in 2004 around 200 million letters were delivered to old addresses. It also touted its new, free service at www.iammoving.com, which allows you to inform companies and other organisations when and where you're moving.

SECURITY MINDED

Store important documents in a lockable filing cabinet or document box. If you must throw away statements, bills and receipts, shred them first (see the box on Shredders on page 212). The same goes for expired credit and debit cards.

Keep the minimum number of cards in your wallet or purse. Should you lose it or have it stolen, you will have fewer cancellation calls to make and thieves will have less personal information to abuse.

When using a card in an ATM, keep an eye out for skimming devices (see the image on page 212). If in doubt, move on to an alternative cash machine or risk having crooks clone your card. When paying by credit card in shops and restaurants, try to keep an eye on your card when it is processed for payment. It should be swiped just once, and only on the till or a portable chip and PIN device.

Finally, don't store PINs on bits of paper in your wallet. If you are worried that you'll forget your number, try adding a false name and number to the contact list in your mobile phone. If you have a Barclaycard with the PIN of 1234 you could store a contact called (for example) Steve Barclay on 01762 841234. It's a good enough memo and, if you are unlucky enough to have both cards and phone stolen, the thief won't be able to jog up to a cashpoint straight away. 

CASE STUDY

A British pensioner on a wine-tasting holiday in South Africa was arrested and thrown in jail for three weeks. Derek Bond had been on Interpol's most wanted list for three years before he was apprehended. The 72-year-old, who authorities believed "may be dangerous", was not involved in property conspiracy, fraud conspiracy or money laundering. But the men who stole his identity 14 years previously might have been.



The FBI had been looking for a suspect going by the names of Derek Bond and Derek Lloyd Sykes. He had the same date of birth and passport number as the real Derek Bond. An anonymous caller informed the FBI of the mistake and Mr Bond was eventually released and received an apology. The FBI tracked down the real criminal in Las Vegas.